Volume 3, Issue 3, March 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Methods to Preserve the Location Privacy in wireless Sensor Network

Prashant Krishan*
I.T. Department
Dehradun Institute of Technology,
Dehradun, India

Abhishek Kumar Chauhan
I.T Department
Dehradun Institute of Technology
Dehradun, India

Abstract— A large growth of location-detection devices results in a wide spread of location-based applications. Examples of Location-based applications include traffic reports, location-based store finders and advertisements. Registered users with location-based services have to send continuously their location to get the answer of their queries. Location-based applications along with the location-based query processing promise safety and convenience, they threaten the privacy and security of their customers. There are many solutions of location privacy in wireless sensor network.

Keywords— Wireless sensor network, casper, anonymity, location anonymization algorithms

I. INTRODUCTION

The explosive growth of location-detection devices (e.g. cellular phones, GPS enabled devices) results in a wide spread of location-based applications. Location-based applications have many examples like location based store finders, traffic reports and location-based advertisements. Registered users with the particular location-based services have to send their location continuously to get the answer of their queries. Although location-based query processing promises safety and convenience, they threaten the privacy and security of their customers. The location-based query processor relies mainly on the implicit assumption that users agree to reveal their private locations. In order to get locations-based services, a user has to report her location. In other words, a user trades her privacy with the services. If a user wants to keep her privacy location information, she has to turn-off her location aware device and (temporarily) unsubscribe from the service. With untrustworthy servers, such model provides several privacy threats. For example, an employer may check on her employee behaviour by knowing the places she visits and the time of each visit, the personal medical records can be inferred by knowing which clinic a person visits, or someone can track the location of ex-friends. In fact, in many cases, GPS devices have been used in stalking personal locations. The traditional approach of pseudononymity means using the fake identity is not applicable to location based applications where a location of a person can directly lead to the true identity. For example, asking about the nearest restaurant to my home using a fake identity will reveal my true identity. In this paper, we will discuss all the proper solutions to remove the privacy issues in WSN.

II. PRIVACY PRESERVING TECHNIQUES

In wireless sensor network, private information collected by sensors and sent through the network and also some context information (location of a sensor initiating communication) is also sent to the base station through a wireless medium. There are some challenges in wireless sensor network like uncontrollable environment in which the defender can't guarantee safety; other challenge is the wireless sensor. Network is resource constraint (its battery life, processing power, memory are limited) and topological constraint e.g. It is responsibility of multiple hops to transmit data to base station and unbalanced traffic patterns can leak contextual information. So these are the constraints by which anyone can trace the private information. The privacy in WSN can be divided in two types Data Privacy, Context Privacy. In Data privacy , if any compromised node is present between the nodes and this node is involved in the routing than the data leakage can be possible. In this category two models can be present external adversary who involves eavesdroppers on communication between nodes and internal adversary, in which any participating node is being captured by the adversary. In Location privacy, the main challenge is to derive the location of base station and data source by observing and analysing the traffic patterns between different hops. Location privacy can also be divided in to two parts data source and base station. In temporal privacy the previously generated messages can be used to predict the next ones. An adversary armed with knowledge of the network deployment, routing algorithms, and the base-station (data sink) location can infer the temporal patterns of interesting events by merely monitoring the arrival of packets at the sink, thereby allowing the adversary to remotely track the spatial -temporal evaluation of a sensed event.

A. Data privacy: In data privacy providing efficient data aggregation while preserving data privacy is a challenging problem in wireless sensor networks research. There are two privacy-preserving data aggregation schemes for additive aggregation functions. The first scheme – Cluster-based Private Data Aggregation (CPDA) – leverages clustering protocol and algebraic properties of polynomials. It has the advantage of incurring less communication overhead. The

second scheme – Slice-Mix-AggRegaTe (SMART) – builds on slicing techniques and the associative property of addition. It has the advantage of incurring less computation overhead.

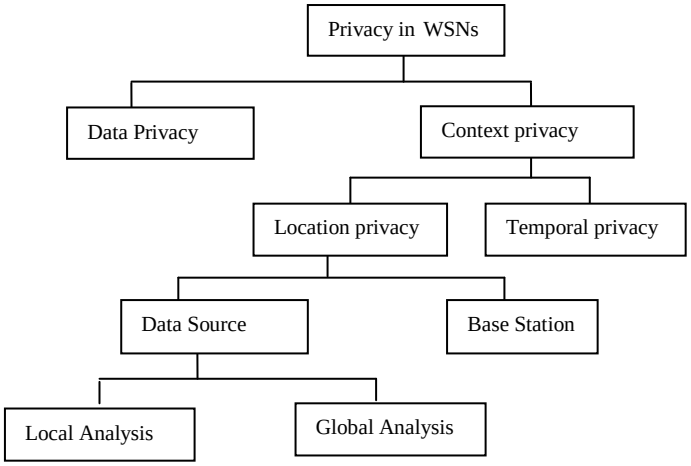

Fig. 1: Categorization of Privacy in WSN

B. Context privacy: context privacy can be further divided into location privacy and temporal privacy.

1. Location privacy: Location privacy is extremely important in WSNs. Information on location of events or on location of base stations can be of a primary concern of an adversary. Suppose the Panda-Hunter Game where a WSN is employed to monitor endangered pandas in their habitat. It is sufficient for the adversary to find out location of sensors currently monitoring the panda to successfully localize and capture the panda. Similarly, the adversary only needs to find out location of the base station to be able to mount a physical or other DoS attack on the base station and thus inactivate the whole network The problem of preserving the location privacy of the sensors of a wireless sensor network when they send a reply to a query broadcast by the BS.

III SOLUTIONS OF LOCATION PRIVACY

There are many solutions available to preserve the location privacy example- anonymity concept, casper system, location anonymization algorithms etc.

A.ANONYMITY CONCEPT: Anonymizing wireless sensor networks allow users to access services privately by using a series of routers to hide the client's IP address from the server. As a result, administrators block all known exit nodes of anonymizing networks, denying anonymous access to misbehaving. To address this problem, servers can "blacklist" misbehaving users, thereby blocking users without compromising their anonymity. Monitoring personal locations with a potentially entrusted server poses privacy threats to the monitored individuals; a privacy-preserving location monitoring system for wireless sensor networks is adopted. Two in network location anonymization algorithms are considered, namely, resource and quality-aware algorithms, which aim to enable the system to provide high-quality location monitoring services for system users, while preserving personal location privacy. Both algorithms rely on the well established k-anonymity privacy concept, that is, a person is indistinguishable among k persons, to enable trusted sensor nodes to provide the aggregate location information of monitored persons. Each aggregate location is in a form of a Monitored area A along with the number of monitored persons residing in A, where A contains at least k persons. The resource-aware algorithm aims to minimize communication and computational cost, while the quality-aware algorithm aims to maximize the accuracy of the aggregate locations by minimizing their monitored areas. To utilize the aggregate location information and to provide location monitoring services, a spatial histogram approach is used that estimates the distribution of the monitored persons based on the gathered aggregate location information. Then, the estimated distribution is used to provide location monitoring services through answering range queries. This module provides security; unauthorized person cannot access the account. Only valid user can access and verify the object moving and object tracking. So we give optional to user can access they account. Protect from the unauthorized users. This system gives protection for the client as well as protects the server.

1) Resource Aware algorithm: The objective of this step is to guarantee that each sensor node knows an adequate number of objects to compute a particular area. To reduce communication cost, this step relies on a heuristic that a sensor node only forwards its received messages to its neighbors when some of them have not yet found an adequate number of objects. Sensor nodes can perform many objects monitoring at the same time.

1.1) *Broadcast Step*: Broadcast step is to guarantee that each sensor node knows an adequate number of objects to compute a cloaked area. To reduce communication cost, this step relies on a heuristic that a sensor node only forwards its received messages to its neighbors when some of them have not yet found an adequate number of objects. In this step, after each sensor node m initializes an empty list Peer List, m sends a with its identity m.ID, sensing area m.Area, and the number of objects located in its sensing area m.count, to its neighbors. When m receives a message from a peer p, m stores the message in its Peer List. Whenever m finds an adequate number of

objects, m sends a notification message to its neighbors. If m has not received the notification message, some neighbors has not found an adequate number of objects, therefore m forwards the received message to its neighbors.

1.2) *Cloaked Area Step*: Cloaked area step is that each sensor node blurs its sensing area into a cloaked area that includes at least k objects to satisfy the k-anonymity privacy requirement. To minimize computational cost, this step uses a greedy approach to find a cloaked area based on the information stored in Peer List.

1.3) *Validation step*: In validation step is to avoid reporting aggregate locations with a relationship to server each sensor node maintains a list to store the aggregate locations sent by other peers. AS this step ensures that no aggregate location with the containment relationship is reported to the server, the adversary cannot obtain any deterministic information from the aggregate locations. Since the server receives an aggregate location from each sensor node for every reporting period, it cannot tell whether any containment relationship takes place among the actual aggregate locations of the sensor nodes.

2) Quality Aware algorithm: In this module, that aim to enable the system to provide high quality location monitoring services for server. This quality aware mechanism finds out the files which are available in the system and they sense even the location of each files.

2.1) *Search Space step*: The search space step is too costly for node m to gather the information of all the sensor nodes to compute its minimal cloaked area. To reduce communication and computational cost, m determines a search space based on the input initial solution. It is to compute the minimal cloaked area.

2.2) *Minimal cloaked Area step*: Minimal cloaked area takes a set of peers in search space, computes the minimal cloaked area for the sensor node. It proposes two optimization techniques to reduce computational cost. The first optimization technique is that need not to examine all the combinations of the peers. This optimization mainly reduces computational cost by reducing the number of computations among the peers. The second optimization technique has two properties 1.Lattice Structure2. Monotonicity Property

2.3) *Validation step*: In validation step is to avoid reporting aggregate locations with a relationship to server. Each sensor node maintains a list to store the aggregate locations sent by other peers. AS this step ensures that no aggregate location with the containment relationship is reported to the server, the adversary cannot obtain any deterministic information from the aggregate locations. Since the server receives an aggregate location from each sensor node for every reporting period, it cannot tell whether any containment relationship takes place among the actual aggregate locations of the sensor nodes as the algorithms send the aggregate location of the network to the base station. And In the data aggregation of WSN, two security requirements, confidentiality and integrity, should be fulfilled. Specifically, the fundamental security issue is data confidentiality, which protects the sensitive transmitted data from passive attacks, such as eavesdropping. Data confidentiality is especially vital in a hostile environment, where the wireless channel is vulnerable to eavesdropping. The complicated encryption and decryption operations, such as modular multiplications of large numbers in public key based cryptosystems, can use up the sensor's power quickly. The other security issue is data integrity, which prevents the compromised source nodes or aggregator nodes from significantly altering the final aggregation value. Sensor nodes are easy to be compromised because the lack expensive tampering-resistant hardware and even that tampering-resistant hardware might not always be reliable. A compromised node can modify, forge or discard messages. Generally, two methods can be used for secure data aggregation in WSN: hop-by-hop encrypted data aggregation and end-to-end encrypted data aggregation. Data is encrypted by the sensing nodes and decrypted by the aggregator nodes. The aggregator nodes then aggregate the data and encrypt the aggregation Result again. Thus any encryption technique can be used to enhance the security (privacy) of the aggregated data.

B.CASPER: Casper mainly consists of two components, namely, the location anonymizer and the privacy-aware query processor. The location anonymizer is a trusted third party that acts as a middle layer between mobile users and the location-based database server in order to: (1) receive the exact location information from mobile users along with a privacy profile of each user, (2) blur the exact location information into cloaked spatial areas based on each user privacy profile, and (3) send the cloaked spatial areas to the location-based data- base server. The privacy-aware query processor is embedded inside the location-based database server to tune its func- tionality to deal with anonymous queries and cloaked spatial areas rather than the exact location information.

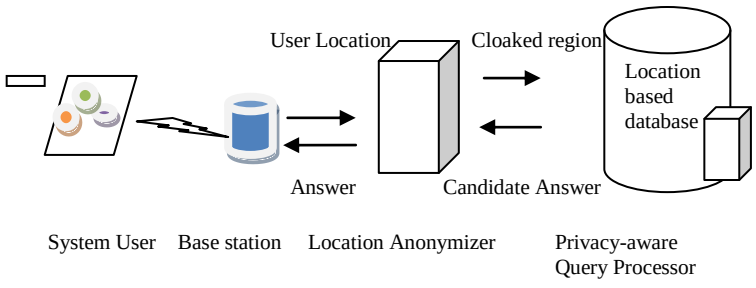

Fig. 2 Casper System architecture

Mobile users register with casper by a certain privacy profile that outlines the privacy requirements of each user. A user privacy profile is defined as a tuple (k,Amin) where k indicates that the user wants to be k-anonymous, i.e. not distinguishable among other k users, while Amin is the minimum acceptable resolution of the cloaked spatial region. Amin is particularly useful in dense areas where even a large k would not achieve higher privacy requirements. Mobile users have the ability to change their privacy profiles at any time. Figure 2 depicts the casper architecture which has two main components: the location anonymizer and the privacy-aware query processor. The location anonymizer receives continuous location updates from mobile users, blurs the location updates to cloaked spatial areas that match each user privacy profile (k, Amin) and sends the cloaked spatial areas to the location-based database server. While cloaking the location information, the anonymizer also removes any user identity to ensure the pseudonymity of the location information. The location anonymizer also blurs the query location information before sending a cloaked query area to the location based data server to anonymously deal with cloaked spatial areas rather than exact point locations. Instead of returning an exact answer, the privacy aware query processor returns a candidate list of answers to the location- based query through the location anonymizer. Mobile users would locally evaluate their queries given the candidate list. The privacy aware query processor guarantees that the exact query answer. The size of the candidate list heavily depends on the user privacy profile. A strictly privacy profile would result in a large candidate list. Using their privacy profiles, mobile users have the ability to adjust a personal trade-off between the amount of information they would like to reveal about their locations and the quality of service that they obtain from casper.

IV CONCLUSION

In this paper we propose the privacy preserving methods for wireless sensor network. Casper– a framework in which mobile users can entertain location-based services without the need to disclose their private location information. Mobile users register with Casper by a user-specified privacy profile. Casper has two main components, the location anonymizer and the privacy-aware query processor. The location anonymizer acts as a third trusted party that blurs the exact location information of each user into a cloaked spatial area that matches the user privacy profile. Resource aware and quality aware algorithm also depicted. In this paper a new idea is also introduced for more privacy. The idea is, when the resource and quality aware algorithm sends the aggregate location and aggregation has confidentiality issues. So the encryption technique can also be used.

REFERENCES:

[1] K. Bohrer, S. Levy, X. Liu, and E. Schonberg, "Individualized Privacy Policy Based Access Control," Proc. Sixth Int'l Conf. Electronic Commerce Research (ICECR), 2003.

[2] E. Snekkenes, "Concepts for Personal Location Privacy Policies," Proc. Third ACM Conf. Electronic Commerce (EC), 2001

[3] L.Ackerman, J. Kempf, and T. Miki. Wireless location privacy:A report on law and policy in the united states, the europrean union, and japan. Technical Report DCL-TR2003-001, DoCoMo Commuinication Laboratories, USA, 2003.

[4] K. Mouratidis, D. Papadias, and M. Hadjieleftheriou.Conceptual Partitioning: An Efficient Method for Continuous Nearest Neighbor Monitoring. In SIGMOD, 2005.

[5] S. _Capkun and J.P. Hubaux, "Secure Positioning in WirelessNetworks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 221-232, Feb. 2006

[6] M. Conti, R.D. Pietro, L.V. Mancini, and A. Mei, "A Randomized,Efficient, and Distributed Protocol for the Detection of NodeReplication Attacks in Wireless Sensor Networks," Proc. ACMMobiHoc, pp. 80-89,
Sept. 2007.

[7] K. Dantu, M. Rahimi, H. Shah, S. Babel, A. Dhariwal, and G.S.Sukhatme,
"Robomote: Enabling Mobility in Sensor Networks,"Proc. Fourth IEEE Int'l Symp Information Processing in SensorNetworks (IPSN), pp. 404-409, Apr. 2005

[8] J. Ho, M. Wright, and S.K. Das, "Fast Detection of Replica Node Attacks in Mobile
Sensor Networks Using Sequential Analysis," Proc. IEEE INFOCOM, pp. 1773- 1781, Apr. 2009.

[9] J. Ho, D. Liu, M. Wright, and S.K. Das, "Distributed Detection of Replicas with Deployment Knowledge in Wireless Sensor Networks," Ad Hoc Networks, vol. 7, no. 8, pp. 1476-1488, Nov. 2009.

[10] L.Hu and D. Evans, "Localization for Mobile Sensor Networks,"Proc. ACM MobiCom, pp. 45-57, Sept. 2004.

[11] J.Jung, V.Paxon, A.W. Berger, and H. Balakrishnan, "Fast Portscan Detection Using Sequential Hypothesis Testing," Proc.IEEE Symp. Security and Privacy, pp. 211-225, May 2004.

[12] Mohamed F. Mokbel, Chi-Yin Chow, Walid G.Aref, " The new casper: Query processing for location Services without Compromising Privacy".

[13] T. Xu and Y. Cai, "Exploring Historical Location Data for Anonymity Preservation in Location-Based Services," Proc. IEEE INFOCOM, 2008

[14] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private Queries in Location Based Services: Anonymizers Are Not Necessary," Proc. ACM SIGMOD, 2008.

[15] W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher, "PDA: Privacy-Preserving Data Aggregation in Wireless Sensor Networks," Proc. IEEE INFOCOM, 2007.

[16] M. Shao, S. Zhu, W. Zhang, and G. Cao, "pDCS: Security and Privacy Support for Data-Centric Sensor Networks," Proc. IEEE INFOCOM, 2007.

[17] B. Carbunar, Y. Yu, W. Shi, M. Pearce, and V. Vasudevan, "Query Privacy in Wireless Sensor Networks," Proc. Fourth Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), 2007.

[18] Brands, "Untraceable Off-Line Cash in Wallets with Observers(Extended Abstract)," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 302-318, 1993.

[19] E. Bresson and J. Stern, "Efficient Revocation in Group Signatures," Proc. Conf. Public Key Cryptography, Springer, pp. 190-206, 2001.

[20] J. Camenisch and A. Lysyanskaya, "An Effic ient System for Non- Transferable Anonymous Credentials with Optional Anonymity Revocation," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), Springer, pp. 93-118, 2001.

[21] J. Camenisch and A. Lysyanskaya, "Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 61-76, 2002.

[22] J. Camenisch and A. Lysyanskaya, "Signature Schemes and Anonymous Credentials from Bilinear Maps," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 56-72, 2004.

